UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/986,319	11/08/2001	Timothy J. Simms	4772-2rwf	5579

23117 7590 07/26/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/986,319	SIMMS, TIMOTHY J.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 May 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,154 and 155* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8, and 154-155* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on May 4, 2007. Claims 154-155 have been added.

2. Claims 1-8, and 154-155 are currently pending consideration.

Response to Arguments

3. Applicant's arguments filed May 4, 2007 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the Applicant argues that the Cited Prior Arts (CPA), Vanstone et al. (U.S. Patent 6,487,660) in view of Bellovin et al. (U.S. Patent 5,241,599), can not be properly combined to teach exchanging a public key in an encrypted message as opposed to obtaining the public key from a trusted third party server as disclosed in Vanstone. This argument is not found persuasive. As stated in the previous Office action, Bellovin discloses exchanging a public key in an encrypted message in order to set up a session key without the involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone. Therefore, it is asserted that the combination is proper, and that it would have been obvious to exchange the public key in an encrypted message as

delineated by Bellovin. Furthermore, the Applicant argues that the CPA does not teach a password. However, Bellovin discloses that the message (Ea) is encrypted using a password (P) as the key resulting in P(Ea) (Bellovin: column 5, lines 23-26). Therefore, it is asserted that a password is taught by the CPA to encrypt the message.

Therefore, the rejection is maintained and applied to the new claims 154-155 as given below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-2, 5 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (U.S. Patent 6,487,660), in view of Bellovin et al. (U.S. Patent 5,241,599).

Regarding claim 1, Vanstone discloses:

A method for establishing secure communication between a calling party and a called party, consisting essentially of:

identifying a first shared random number associated with a calling party (column 3 lines 35-42), wherein x is the first random number;

identifying a second random number associated with a called party (column 3 lines 42-44), wherein y is the second random number;

identifying said calling party to said called party (column 3 lines 45-53), wherein an identification string is sent from the ATM to the server;

generating a public-private key pair by said called party (column 5 lines 1-10), wherein the server generates its private-public key pair;

transmitting a second message from said calling party to said called party, said second message including said second shared random number, and said second message (column 3 lines 55-56) and

obtaining a shared secret key from an output of a combining function having a first input including said first shared random number and having a second input including said second shared random number (column 6 lines 25-30).

Vanstone does not explicitly disclose transmitting a first message from the called party to the calling party wherein the first message includes a first random number and the public portion of the public-private key pair. Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5 lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a

password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone.

Furthermore, Vanstone does not disclose that the second message is encrypted with the public key. Bellovin discloses that a message containing a random number is encrypted with a public key (column 5 lines 33-38). Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. It would have been obvious to one of ordinary skill in the art at the time of invention use a public key to encrypt the message in order to secure the exchange of the parameters so that a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Vanstone discloses:

The method of claim 1, wherein said combining function includes a logical function (column 3 lines 52-62).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Vanstone discloses:

The method of claim 1, further comprising the step of transmitting a second message from said second computer to said first computer, said second message including said second shared random number (column 3 lines 55-56).

Claim 9 is rejected as applied above in rejecting claim 5. Vanstone does not disclose wherein the first message includes an asymmetric key. Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5 lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the

involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone.

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (U.S. Patent 6,487,660), in view of Bellovin et al. (U.S. Patent 5,241,599) in further in view of Shona et al. (U.S. Patent 6,018,581).

Claim 3 is rejected as applied above in rejecting claim 2. Vanstone-Bellovin does not explicitly disclose that the logical function is an XOR function. Shona discloses a method wherein the logical function is an exclusive-or (XOR) function (column 6 lines 12-16, lines 22-25). It would have been obvious to one of ordinary skill in the art at the time of invention to combine the teachings of Shona with the teachings of Vanstone-Bellovin to make the encryption key greatly varied (column 6 lines 25-29).

6. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (U.S. Patent 6,487,660), in view of Bellovin et al. (U.S. Patent 5,241,599) in further in view of Wu (U.S. Patent 6,539,749).

Regarding claims 6-8, Vanstone does not explicitly disclose wherein the first message is encoded using a password. Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5 lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone. However, the password is not encoded/encrypted. Wu teaches that the password is an encoded password (column 3 lines 33-37). Wu, Vanstone and Bellovin are all analogous arts as they are all concerned with setting up a secure communication channel via a session key. It would have been obvious to one of ordinary skill in the art at the time of invention to have combined the teachings of Vanstone-Bellovin, with the

teachings of Wu, in order to verify a user's asserted password without having to reveal the user's password (column 3 lines 35-37).

Regarding claim 154, Vanstone discloses:

A method for establishing secure communication between a calling party and a called party, comprising:

generating, on demand at the called party, an asymmetric key pair including a public and a private key (column 5 lines 1-10), wherein the server generates its private-public key pair;

said calling party receiving and decrypting said first encrypted message using said symmetric encryption key to obtain said first random number and said public key (column 5, lines 33-37), wherein Bob decrypts the message to get the message;

said calling party transmitting, to said called party, a second encrypted message including a second random number, said calling party encrypting said second message with said public key of said asymmetric key pair (column 3, lines 55-56);

said called party receiving and decrypting said second encrypted message to obtain said second random number (column 5, lines 41-45), wherein R or numbers derive from R are used as a key;

said calling and called parties each independently applying said no-shared first and second random numbers to combing functions to thereby each independently generate a shared secret key (column 6, lines 25-30);

said calling and called parties encrypting further communications therebetween at least in part using said shared secret key (column 5, lines 32-45), wherein the key is used in further communications between Alice and Bob.

Vanstone does not explicitly disclose transmitting a first message from the called party to the calling party wherein the first message includes a first random number and the public portion of the public-private key pair. Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5 lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone.

Vanstone does not explicitly disclose wherein the first message is encoded using a symmetric encryption key (password). Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5 lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone

Claim 155 is rejected as applied above in rejecting claim 154. Vanstone does not explicitly disclose wherein the first message is encoded using a password. Bellovin discloses a system of bi-directional secure communication where a public key is sent from a sender to a receiver, the public key being encrypted with a password (column 5

lines 18-32). Bellovin uses this exchange to set up a session key to be used for encrypting bi-directional communications between sender and receiver. Vanstone and Bellovin are analogous arts as both are concerned with setting up a secure communication channel between a sender and a receiver. Bellovin transmits the public key encrypted with a password from a sender to a receiver in order to set up a session key for bi-directional communications. In Vanstone, the public keys are either built into the devices, or transmitted by a third party (column 5 lines 1-24). It would have been obvious to one of ordinary skill in the art at the time of the invention use the method of Bellovin to transmit the public key to the calling party in order to set up a session key without the involvement of a third party which would allow the set up of a private and authenticated communication between parties that only share a secret, while avoiding the costs and restrictions of prior cryptographic protocols (column 3 lines 52-62) such as a third party controlling key distribution as delineated in Vanstone

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KA 7/22/07

KA
07/22/2007

CHRISTOPHER REVAK
PRIMARY EXAMINER